Computer Security Expert Assist Team

CSEAT

Joan Hash, (301) 975-3357

joan.hash@nist.gov

Information Technology Laboratory

National Institute of Standards and Technology

http://cseat.nist.gov

cseat@nist.gov

NIST

National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

CSEAT Purpose

- **Assist agencies/programs in improving the security of Federal IT systems**
  - Strengthen security of critical computer system/services
  - Identify security program issues and provide specific remedies
  - Prepare for future security threats
- **Improve federal agency/program Critical Infrastructure Protection (CIP) planning and implementation efforts**
- **Identify and develop appropriate computer security guidelines**

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Why NIST?

- NIST provides consistent, comparable, and neutral perspective
- As a result of the review process, NIST obtains better understanding of Federal agency/program needs for guidelines
- Effort helps NIST meet statutory responsibilities
  - Provide technical assistance in implementing standards and guidelines, including:
    - Case studies
    - Lessons learned
    - Quick references
    - Checklists

CSEAT Complements Existing Efforts

- **Government**
  - NIST standards and guidelines
  - Federal Computer Incident Response Capability (FedCIRC) /Computer Emergency Response Teams (CERTs)
  - National Infrastructure Protection Center (NIPC)
  - Critical Infrastructure Assurance Office (CIAO)
  - NSA security evaluations
  - GSA's security contract vehicles
- **Industry**
  - Information Sharing and Analysis Centers (ISACs)

CSEAT Review Types

2 types of reviews

- **Agency requested review of automated information security programs**
- **Agency program and OMB requested high-risk IT program security reviews**
  - Both existing and planned programs
  - E.g. child welfare, disaster relief, Indian trust management

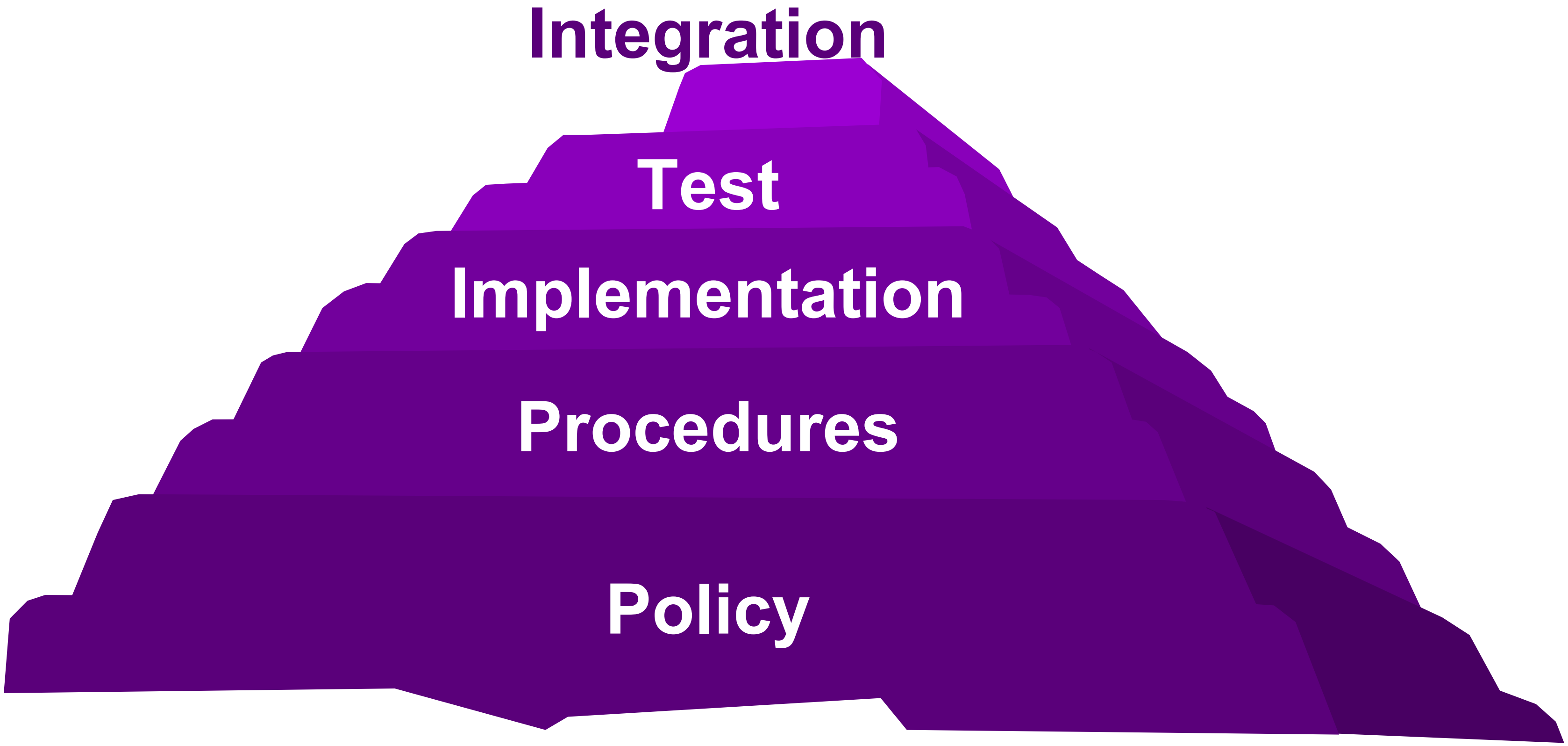
Computer Security Expert Assist Team
CSEAT

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CSEAT Review

- **CSEAT security control objectives abstracted directly from long-standing requirements from**
  - Federal government regulations
  - Statutes
  - Policies
  - Guidelines
- **CSEAT provides an independent review of an agency's IT security program or high risk program**
  - Agency requested - not an audit
  - Assesses the state of maturity of the agency's or program's IT security policy and procedure implementation and overall integration
- **Restricted to unclassified information/systems**

CSEAT Review Maturity Levels



Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CSEAT Review Topic Areas

- Computer security management and culture
- Computer security plans
- Security awareness, training, and education
- Budget and resources
- Life cycle management
- Incident and emergency response
- Operational security controls
- Physical security
- IT security controls

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Computer Security Management and Culture Subtopic Areas

- IT roles and responsibilities
- Review of security controls
- Rules of behavior and documentation
- Performance assessment and feedback
- Critical infrastructure protection
- Personnel controls

High risk program only:

- Program specific controls

Computer Security Plans Subtopic Areas

- System security plan
- Risk management
- Authorized processing
- Documentation

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Security Awareness, Training, and Education Subtopic Areas

- End users' security awareness and training
- IT professionals' security awareness and training
- Management security awareness and training

High risk program only:

- Program specific security training

Budget and Resources Subtopic Areas

- IT security - part of capital planning process
- Adequate resources applied to IT security
- IT security funding and resources distributed based upon a risk model
- Cost effective IT security solutions
- Procurement controls

Life Cycle Management Subtopic Areas

- System development life cycle (SDLC) methodology
- Changes controlled and tested through SDLC

High risk program only:

- Security requirements definition
- Security design
- Security implementation
- Security testing
- Security deployment

Incident and Emergency Response

Subtopic Areas

- Critical and sensitive assets identification
- Contingency/disaster response
- Incident identification, reporting, and response
- Continuity of operations

Operational Security Controls

Subtopic Areas

- Hardware and systems software maintenance
- Data integrity
- Production I/O
- Data confidentiality
- Data availability
- Systems operations documentation

Physical Security Subtopic Areas

- Implementation of physical security controls
- Personal electronic device protection
- Emanation controls
- Temporary controlled facility controls

IT Security Controls Subtopic Areas

- Identification and authentication
- Logical access controls
- Auditing

Review Elements

- Each subtopic area is composed of many review elements
- Each review element broken down into 5 maturity levels
- Each maturity level determined for each review element
  - Complete
  - Partially complete
  - Not started
- Higher maturity level cannot be more complete than lower level

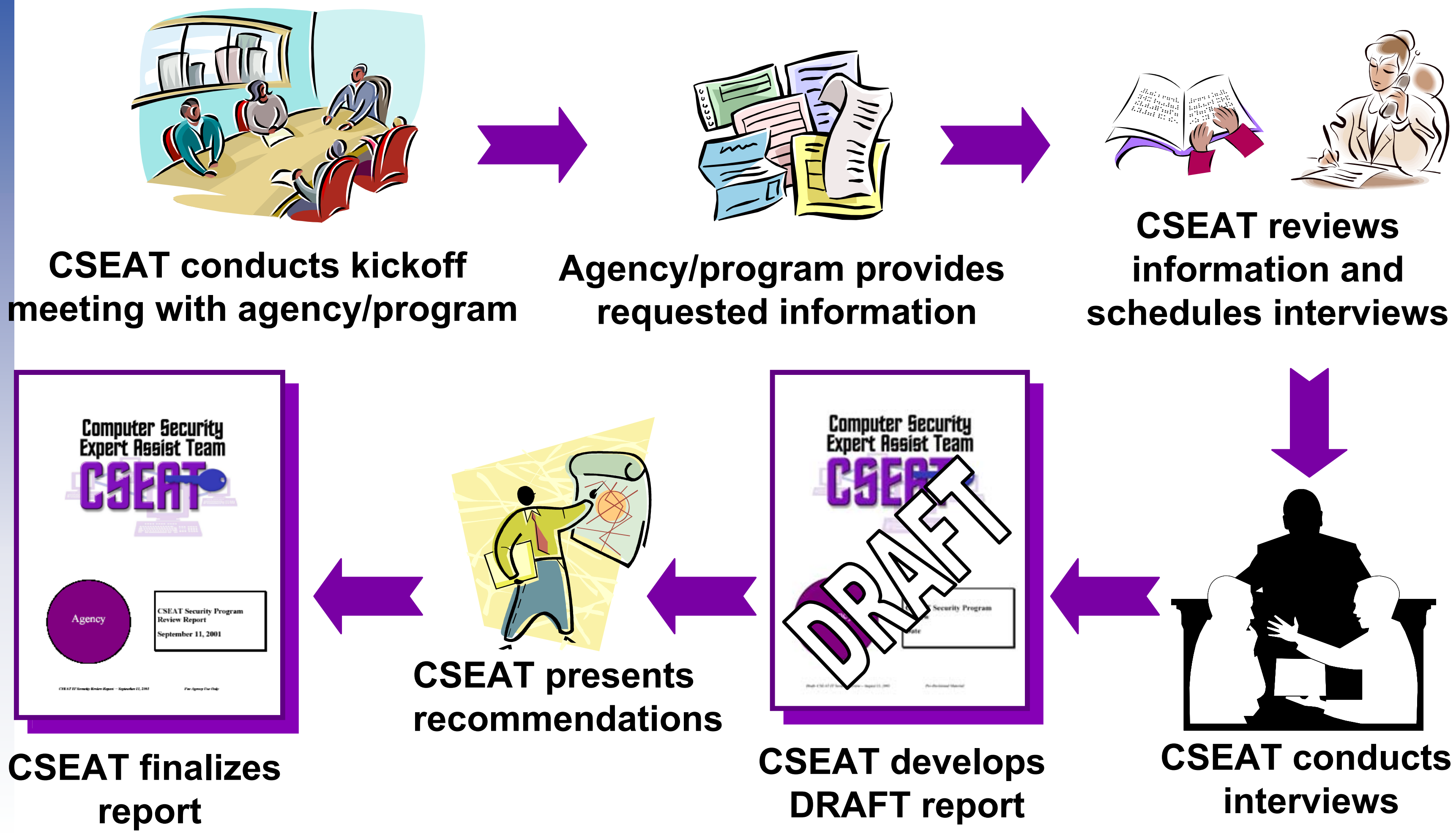
Element Example for IT Security Controls

- **Subtopic area - Logical Access Controls**
- **Element:**
  - Are insecure protocols (e.g., UDP, ftp, etc.) disabled?
- **Maturity levels:**
  - Is there a policy requiring disabling of protocols?
  - Are there procedures for disabling protocols?
  - Are insecure protocols disabled?
  - Have tests been conducted to verify that insecure protocols are disabled?
  - Is disabling insecure protocols standard business practice?

Element Example for Computer Security Management and Culture

- **Subtopic area - Critical Infrastructure Protection**
- **Element:**
  - Have all business partners developed and agreed to interconnection agreements?
- **Maturity levels:**
  - Is there a policy that requires these agreements?
  - Are there procedures to develop and agree?
  - Has this been done?
  - Are there periodic reviews to verify that this has been done for all interconnections?
  - Is this now part of the general business practice of the organization?

CSEAT Agency/Program Review Process


Computer Security Expert Assist Team
CSEAT
DRAFT
Computer Security Expert Assist Team
CSEAT
Agency
CSEAT Security Program Review Report
September 11, 2001

CSEAT conducts kickoff meeting with agency/program

Agency/program provides requested information

CSEAT reviews information and schedules interviews

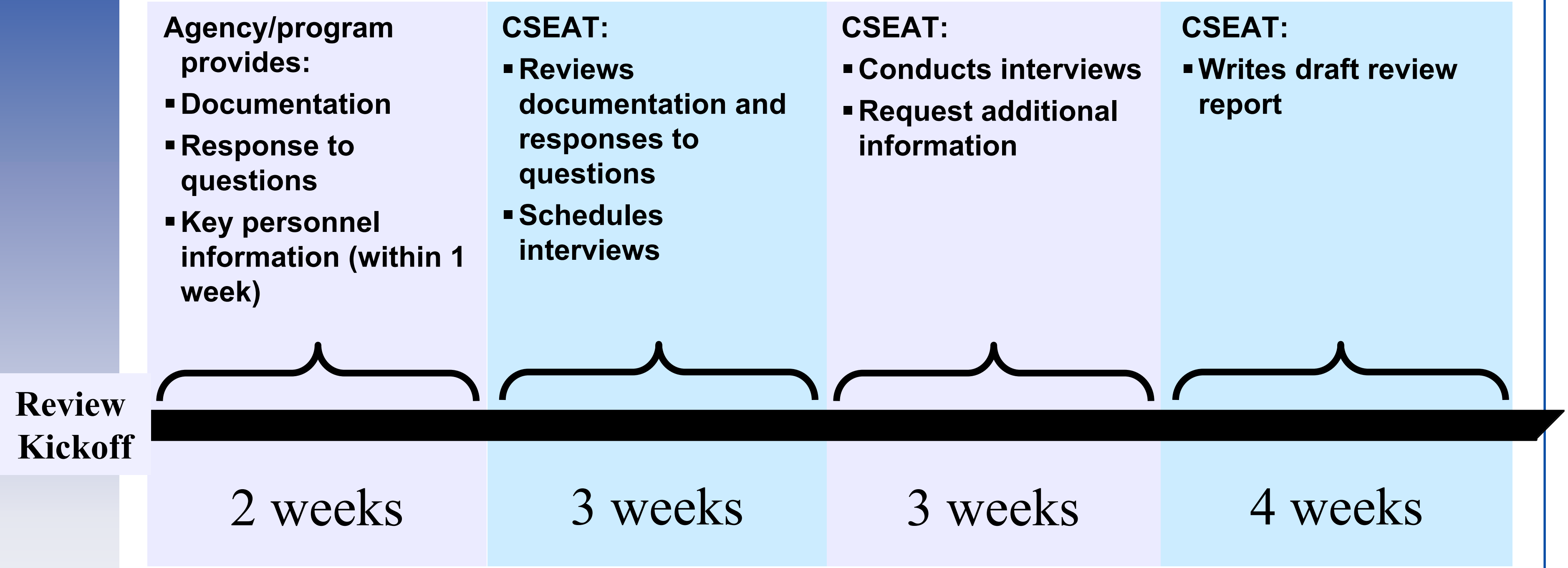
CSEAT conducts interviews

CSEAT develops DRAFT report

CSEAT presents recommendations

CSEAT finalizes report

Proposed Review Timeline



Review Kickoff	Agency/program provides: ▪ Documentation ▪ Response to questions ▪ Key personnel information (within 1 week)	CSEAT: ▪ Reviews documentation and responses to questions ▪ Schedules interviews	CSEAT: ▪ Conducts interviews ▪ Request additional information	CSEAT: ▪ Writes draft review report
	2 weeks	3 weeks	3 weeks	4 weeks

Agency/program provides comments on draft – 30 days after receipt of draft
CSEAT provides final review report – 14 days after receipt of comments

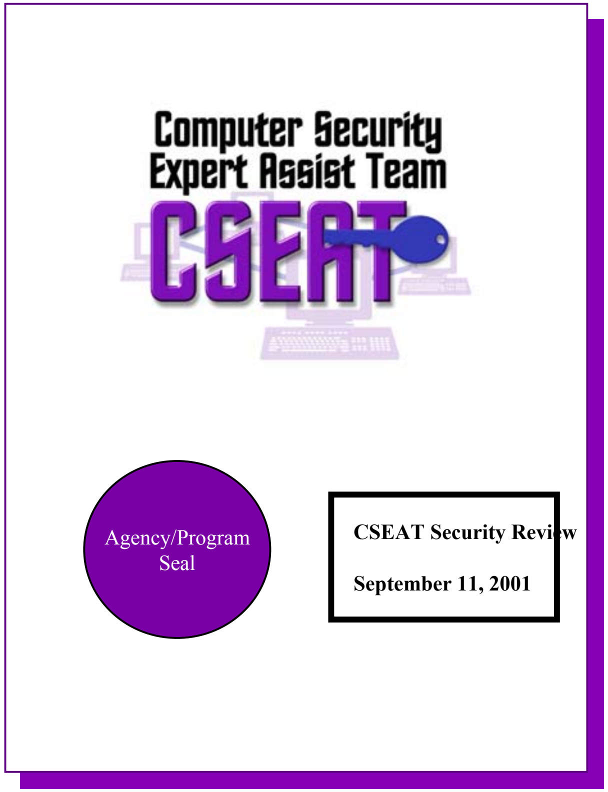
Timeline phase duration is dependent upon completion of previous phase.

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CSEAT Review Report

- CSEAT overview
- Agency or program overview
- Agency or program status
- Recommendations to improve agency or program computer security
- Summary and conclusions
- Prioritized, implementable action plan



Computer Security Expert Assist Team

CSEAT

Agency/Program Seal

CSEAT Security Review

September 11, 2001

Agency or Program IT Security Status

(Sample)

	Policy	Procedures	Implementation	Testing	Integration
Computer Security Management and Culture	🟨	🟨	🟨	🟥	🟥
Computer Security Plans	🟨	🟨	🟨	🟥	🟥
Security Awareness, Training, and Education	🟩	🟨	🟨	🟥	🟥
Budget and Resources	🟨	🟨	🟨	🟥	🟥
Life Cycle Management	🟩	🟩	🟨	🟥	🟥
Incident and Emergency Response	🟨	🟨	🟨	🟥	🟥
Operational Security Controls	🟩	🟨	🟨	🟥	🟥
Physical Security	🟨	🟨	🟨	🟥	🟥
IT Security Controls	🟨	🟨	🟨	🟥	🟥

Compliant	🟩
Partially Compliant	🟨
Not Compliant	🟥

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Issue Identification with Corrective Actions

Issue: Information and systems are endangered due to a failure to manage access rights and accounts for agency employees.

Discussion:

- User accounts are not removed immediately upon user termination.
- Reassigned personnel still retain account access for previous position.

(Sample)

Corrective Actions:

Implement a process to provide accountability for user account creation, deactivation, activation, and termination on all systems in a timely manner.

- Cost – Minimal
- Time to Complete – Short-term
- Recurring Cost – Minimal
- Recurring Time to Complete – Short-term

Computer Security Expert Assist Team CSEAT

NIST National Institute of Standards and Technology Technology Administration U.S. Department of Commerce

Prioritized Action Plan

- **Action priority and topic area**
- **Issue**
- **Suggested corrective action**
- **How long to complete initial action**
  - Short Term = less than 6 months
  - Intermediate Term = between 6 months and 2 years
  - Long Term = more than 2 years
- **Cost to complete initial action**
  - Minimal = Less than $100,000
  - Moderate = Between $100,000 and $500,000
  - High = Greater than $500,000
- **Recurring action time and cost to complete**

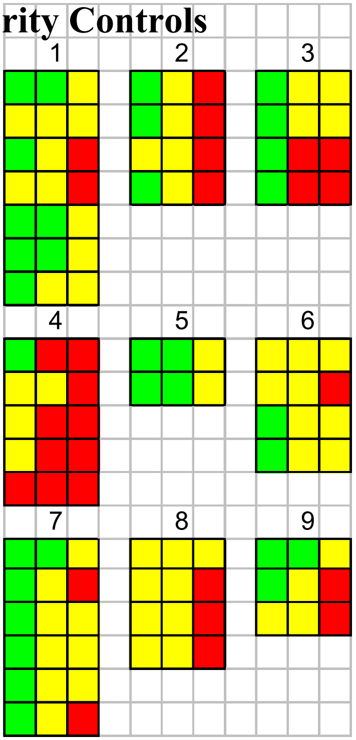
Change in Computer Security Posture after $2 Million Action Plan

CSEAT Review Areas

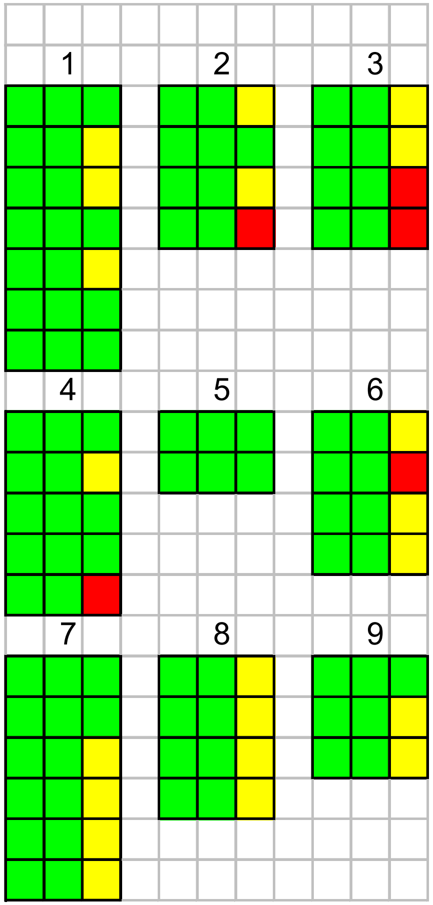
1. Computer Security Management and Culture
2. Computer Security Plans
3. Security Awareness, Training, and Education
4. Budget and Resources
5. Life Cycle Management
6. Incident and Emergency Response
7. Operational Security Controls
8. Physical Security
9. IT Security Controls

(Sample)

Current Status



$2 M Invested



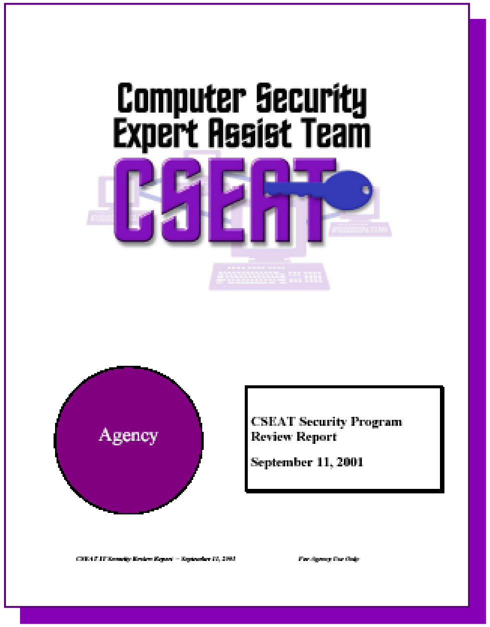
Computer Security Enhancements

- Complete policies
- Complete procedures
- Increase documentation
- Develop and implement capital planning process
- Augment employee training
- Implement computer security plans
- Develop risk assessment methodology
- Develop performance metrics

Computer Security Expert Assist Team
CSEAT

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CSEAT Uses Report to Develop Guidelines



Computer Security
Expert Assist Team
CSEAT

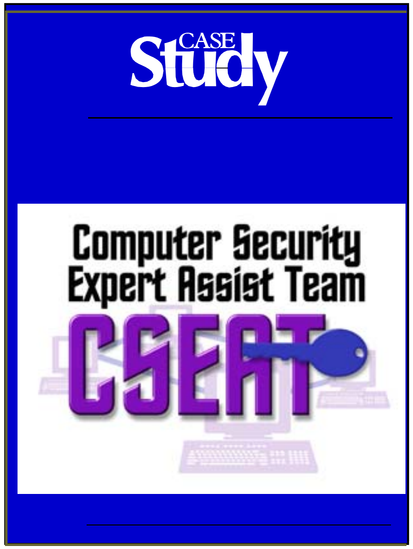
Agency

CSEAT Security Program
Review Report

September 11, 2001

CSEAT IT Security Review Report – September 11, 2001 *For Agency Use Only*

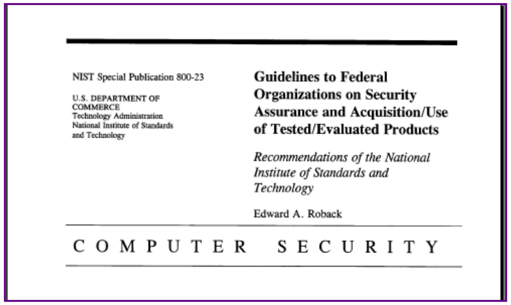
CSEAT Review Report with Recommendations



CASE
Study

Computer Security
Expert Assist Team
CSEAT

Sanitized Case Study



NIST Special Publication 800-23

U.S. DEPARTMENT OF
COMMERCE
Technology Administration
National Institute of Standards
and Technology

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Edward A. Roback

COMPUTER SECURITY

NIST Guidelines

Computer Security
Expert Assist Team
CSEAT

Common IT Security Issues

- **Lack of formalization**
  - Bob knows how to do it
  - Alice keeps the server secure
  - We all know what has to be done and don’t need it written down
- **Impact**
  - Single point of failure
  - Work waits until employee returns
  - Employee retires and new person doesn’t know what has been done
  - Little ability to recover from disaster

Common IT Security Issues (continued)

- **Policies and/or procedures not defined**
  - Different groups independently decide on a policy
  - Different groups implement IT security differently
  - Inconsistent interpretation and implementation across organization/program
- **Impact**
  - Interpretation and implementation may not reflect real organizational/program requirements
  - Difficult to identify the cause of problems
  - Inconsistency leads to increased costs

Common IT Security Issues (continued)

- **Capital planning process missing IT security**
  - IT security not addressed as a primary component
  - Performance measures not included
  - Cost-effectiveness of IT security solutions not addressed
- **Impact**
  - Budgets may be cut or redirected
  - Adequate resources may not be applied to IT security
  - Implemented IT security solutions may not be cost-effective

Common IT Security Issues (continued)

- **IT security considered “their” problem**
  - IT security issues provided to IT security personnel
  - IT security responsibility and accountability not considered part of every employee’s performance
- **Impact**
  - Critical system security may be insufficient
  - Lack of ownership of security issues
  - Vulnerabilities increase over time
  - Security expenditures may be higher than necessary due to “faulty” integration into the life cycle management process

Common IT Security Issues
(concluded)

- **Lack of sufficient training**
  - Employees don’t understand their role in IT security
  - Current threats not addressed
  - IT security not a primary concern for employee
  - Systems not updated with current security patches
- **Impact**
  - Employees indulge in poor security practices
  - Systems vulnerable
  - New and updated systems insecure

Benefits of High Level IT Security Review

- Without the basic IT security infrastructure, it is virtually impossible to have effective IT security.
- Independent and neutral third party can more readily identify IT security issues.
- NIST has extensive knowledge of relevant legislation, standards, and guidelines and can identify issues and corrective actions.
- NIST is able to provide appropriate guidelines in a timely manner.

OMB Identified Criteria*

To ensure that security is addressed throughout the budget process

- Agencies must report security costs for each major and significant IT investment.
- Agencies must document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment.
- Agency security reports and corrective action plans are presumed to reflect the agency's security priorities and thus will be a central tool for OMB in prioritizing funding for systems.
- Agencies must tie their corrective action plans for a system directly to the business case for that IT investment.

*From OMB FY 2001 Report to Congress on Federal Government Information Security Reform, February 13, 2002

Contact Information

Joan Hash

(301) 975-3357

joan.hash@nist.gov

Information Technology Laboratory

National Institute of Standards and Technology

URL: http://cseat.nist.gov

Email: cseat@nist.gov